ARBONIA

IT SECURITY

Bulletin o bezpečnosti informácií

Smernica o heslách

Verzia	1.0
Schválená dňa:	08.07. 2021
Stav:	RELEASED
Klasifikácia:	RESTRICTED
Vypracoval:	ICT Security Officer
Schválil:	Arbonia IT Board
Smernica:	IS-ISP-GROUP-001-PASSWORD-POLICY_SK
Revízia:	neuvedené

Informácie o smernici

Účel	Smernica o heslách popisuje a definuje princípy pre vytváranie, prácu a používanie hesiel v spoločnosti Arbonia.
Používateľ/príjemca	▪ Všetky zamestnanci spoločnosti Arbonia AG ▪ Externí dodávatelia/poskytovatelia služieb/zákazníci a partneri, ktorí majú prístup do systémov ICT spoločnosti Arbonia
Elektronické ukladanie dokumentov	https:\\security.arbonia.com

Vykonané zmeny

Verzia	Dátum	Stav	Zmena	vykonal
0.1	2021-06-14	Draft	Draft of the policy	ICT Security Officer
0.9	2021-07-07	Draft	Draft for adoption	ICT Security Officer
0.9	2021-07-07	Review		Arbonia IT Board
1.0	2021-07-08	Adoption		Arbonia IT Board

Obsah

Zoznam skratiek

Pojem	Popis
ICT	Informations and Communications Technology (informačná a komunikačná technika)
OS	Operating System (operačný systém)
ISMS	Systém riadenia informačnej bezpečnosti

Slovník

Pojem	Popis
Útok Brute Fore	Útok Brute Force je pokus o prelomenie hesla alebo používateľského mena vyskúšaním všetkých možností.
Systém riadenia informačnej bezpečnosti	Systém riadenia informačnej bezpečnosti je vytvorenie postupov a pravidiel v rámci organizácie, ktoré slúžia na trvalé definovanie, riadenie, kontrolu, udržiavanie a neustále zlepšovanie informačnej bezpečnosti.

1 Účel, oblasť použitia a používateľ

Smernica popisuje požiadavky a špecifikácie hesiel pre prístup do systémov ICT spoločnosti Arbonia. Stanovuje pravidlá bezpečného riadenia, používania a vytvárania hesiel.

Smernica sa vzťahuje na celú oblasť použitia systému riadenia informačnej bezpečnosti (ISMS), t. j. na všetky systémy ICT spoločnosti Arbonia.

Používateľmi a príjemcovia tejto smernice sú všetci zamestnanci spoločnosti Arbonia, ako aj dodávatelia/poskytovatelia služieb/zákazníci a partneri, ktorí potrebujú prístup do systémov ICT spoločnosti Arbonia.

2 Princípy Governance

2.1 Dôležitosť hesiel

Bezpečnosť systémov ICT spoločnosti Arbonia je okrem iného založená na starostlivom zaobchádzaní s heslami a predovšetkým na dodržiavaní základných zásad používania hesiel.

Jedným z hlavných cieľov útočníkov je ukradnúť prihlasovacie údaje používateľa, aby získali prístup do systémov ICT spoločnosti Arbonia a následne našli a využili možné slabé miesta. Snažia sa získať privilegované oprávnenia administrátora systému, pomocou ktorých môžu v najhoršom prípade nepozorovane vykonávať rôzne činnosti, ako je napr. krádež údajov, špionáž alebo inštalácia škodlivého softvéru. Z tohto dôvodu predstavujú slabé heslá, ako aj nesprávna manipulácia s nimi značné riziko. Toto riziko sa ďalej zvyšuje pri nevyhnutnom používaní privilegovaných oprávnení, ktoré sú často potrebné na vykonávanie pracovných činností.

Preto je nevyhnutné zabrániť krádeži prístupových údajov a dodržiavať nasledujúce povinnosti.

2.2 Povinnosti používateľa/majiteľa účtu

Všetci používatelia musia pri výbere a používaní hesiel dodržiavať osvedčené a bezpečné postupy (viac informácií nájdete v kapitole 3):

- Vždy sa musí zvoliť «silné heslo». Dĺžka a formát hesla musia byť zvolené tak, aby bol útok Brute Force časovo náročný a neviedol k úspechu
- Heslá sa nesmú prezradiť iným osobám. Taktiež nie nadriadeným, vedeniu spoločnosti alebo administrátorom systému
- Heslá sa nesmú zapisovať ani nevhodne ukladať (napr. v programe Excel), ak oddelenie IT neschválilo na tento účel bezpečnú metódu (napr. nástroj na ukladanie hesiel)
- Heslá sa musia meniť v pravidelných intervaloch
- Heslá sa musia zmeniť, ak hrozí, že boli prezradené, t. j. sprístupnené tretím stranám
- Náznaky zneužitia sa musia okamžite nahlásiť zodpovednému oddeleniu IT
- Ak má používateľ/ka vyhradené používateľské konto s oprávneniami administrátora, nesmie používať rovnaké heslo ako pre štandardný účet
- Majiteľ účtu je v každom prípade zodpovedný za dodržiavanie smernice o heslách, aj keď to nie je možné technicky vynútiť. V žiadnom prípade by sa nemali používať predvolené, prázdne alebo slabé heslá

3 Smernica o heslách

3.1 Definícia

Na dosiahnutie primeranej úrovne informačnej bezpečnosti sa uplatňujú rôzne smernice o heslách v závislosti od požadovaných oprávnení. Rozlišuje sa medzi:

- Všeobecným používaním typu «Používateľ», bez oprávnení administrátora pre systémy ICT
- Špecifickým používaním typu «Administrátor», s oprávneniami administrátora pre jeden alebo viaceré systémy ICT. Rozlišujú sa nasledujúce účty typu «Administrátor»:
    - Služobné/systémové/servisné účty (používajú sa na automatizované funkcie, inštaláciu alebo správu komponentov v systémoch ICT, ako sú OS, databázy, aplikácie alebo sieťové účty atď.)
    - Účty administrátorov (používajú sa pre jednotlivcov, aby mali privilegovaný prístup do systémov ICT)

3.2 Riadenie hesiel

1. Heslo je priradené jedinečnému ID účtu (používateľa alebo administrátora)
2. ID, ako aj heslo sú osobné. Heslo je známe len zodpovednej osobe.
3. Heslo sa nesmie ukladať ako obyčajný text
4. Platnosť hesla nesmie nikdy presiahnuť 360 dní, príp. 540 dní (pozri kapitolu 3.3)
5. Nové heslo bude odmietnuté, ak sa nachádza medzi poslednými 5 použitými heslami
6. Počet neúspešných pokusov o zadanie hesla je obmedzený na 6. Po šiestom pokuse bude účet zablokovaný, kým ho administrátor opäť neodblokuje.
7. Počítadlo neúspešných pokusov o prihlásenie sa nesmie vynulovať za menej ako 60 minút
8. Dočasné heslá môžu mať platnosť < 72 hodín a používateľ musí byť pri prvom prihlásení vyzvaný na zmenu dočasného hesla. To platí, ak je to technicky možné. Ak nie, každý majiteľ účtu je sám zodpovedný za zmenu hesla
9. Automatické pridelenie hesla pri otvorení používateľského účtu sa vykonáva podľa rovnakých špecifikácií

Osobitný predpis pre služobné/systémové/servisné účty:

- Výnimka z pravidla č. 2: heslá spojené s týmto typom účtu sa môžu uchovávať v bezpečnom (šifrovanom) nástroji s prístupom chráneným heslom a zdieľať s viacerými osobami prostredníctvom definovaných skupín funkcií a oprávnení, ak je to potrebné na vykonávanie ich práce
- Výnimka z pravidla č. 4: heslá spojené s týmto typom účtu môžu mať v prípade potreby povolenú možnosť, že nikdy nevyprší platnosť hesla
- Výnimka z pravidla č. 6: heslá spojené s týmto typom účtu nemusia byť automaticky blokované

Spracovanie výnimiek nájdete v kapitole 3.5.

3.3 Vytváranie hesiel

Heslo pre účet typu «Používateľ», bez oprávnení administrátora pre systémy ICT, musí zodpovedať nasledujúcim požiadavkám:

- Obsahuje minimálne 12 znakov pre heslo s platnosťou 360 dní, príp. minimálne 16 znakov pre heslo s platnosťou 540 dní
- Má zložitosť 4 zo 4, čo znamená, že nasledujúce znaky musia byť použité aspoň raz:
    - Veľké písmená
    - Malé písmená
    - Čísla od 0 po 9
    - Interpunkčné znamienka alebo špeciálne znaky (nie všetky systémy ICT akceptujú všetky znaky)
- Nesmie obsahovať názov účtu
- Nesmie obsahovať čísla na prvom a poslednom mieste
- Nesmie obsahovať 3 po sebe idúce rovnaké znaky

Pre heslá typu «Administrátor», s oprávneniami administrátora pre systémy ICT, platia dodatočne nasledujúce osobitné predpisy:

Osobitný predpis pre služobné/systémové/servisné účty:

- Obsahuje minimálne 32 znakov
- Heslo musí byť náhodne vygenerované a zdokumentované pomocou vhodného nástroja na zadávanie hesiel (pozri výnimku z pravidla č. 2, kapitola 3.2)

Osobitný predpis pre administrátorské účty:

- Obsahuje minimálne 15 znakov

Osobitný predpis pre systémy tretích strán (B2C/B2B a iné) prevádzkované spoločnosťou Arbonia:

Špecifikácie hesla sa vzťahujú aj na systémy tretích strán, ale v prípade potreby ich možno prispôsobiť príslušnému obchodnému prípadu použitia. V každom prípade sa osobitné predpisy musia riešiť podľa kapitoly 3.5.

Osobitné požiadavky na účty systému Windows – interné a automaticky vytvárané v spoločnosti Arbonia

- Nové nastavené heslo nesmie existovať v databáze s kompromitovanými heslami. Tomu zabráni technická kontrola pri vytváraní hesla
- Nové nastavené heslo sa nesmie vyskytovať v používateľom definovanom slovníku. Tento slovník sa vedie centrálne a okrem iného obsahuje názov spoločnosti. Zakázané slová sa zobrazia priamo v prípade zhody
- Heslo sa musí zmeniť, ak sa objavilo v databáze kompromitovaných hesiel

3.4 Stratégia vytvárania hesiel

História hesiel	5
Maximálna platnosť hesla	360 (12 – 15 znakov), príp. 540 dní (≥ 16 znakov)
Minimálna platnosť hesla	0
Zložitosť	4/4 (veľké/malé písmená/číslice 0 – 9/interpunkčné znamienka alebo špeciálne znaky)
Minimálna dĺžka hesla o Používateľ o Služobné/systémové/servisné účty o Administrátorské účty	 12 znakov 32 znakov (náhodne generované) 15 znakov
Reverzné šifrovanie (doména systému Windows)	deaktivované
Počet neúspešných pokusov o prihlásenie, kým sa účet zablokuje	6
Trvanie blokovania účtu	Do odblokovania administrátorom
Trvanie do vynulovania počítadla neúspešných pokusov o prihlásenie	≥ 60 minút
Špeciálne (doména systému Windows)	Heslo nesmie obsahovať žiadne čísla na prvom a poslednom mieste Heslo nesmie obsahovať 3 po sebe idúce rovnaké znaky

3.5 Výnimky/špeciálne

Všetky počítačové postupy overovania totožnosti musia v čo najväčšej možnej miere implementovať a overovať súlad s požiadavkami tejto smernice. Ak chýbajú technické požiadavky na implementáciu, musí ich zabezpečiť príslušný majiteľ účtu manuálnym postupom a v rámci možností systému sa musí používať silné heslo.

Lokálny bezpečnostný pracovník IT môže udeliť výnimky z tejto smernice, ak sú dodržané zásady informačnej bezpečnosti a neexistuje riziko pre systémy ICT spoločnosti Arbonia. Ten rozhodne v prípade potreby po konzultácii s bezpečnostným referentom ICT, či udelí výnimku alebo určí ďalšie opatrenia na minimalizáciu rizika. Všetky výnimky sa musia písomne zaznamenať do zoznamu.

4 Vytváranie silných hesiel

Existuje niekoľko techník na vytvorenie a zapamätanie silného hesla:

Príklad 1: vytvorenie silného hesla na základe vety

Vyberte si vetu, ktorú si dobre pamätáte, a pretvorte ju na heslo.

Príklad: Nie je až také zložité vybrať si silné heslo.

Použite prvé písmená alebo niekoľko písmen jednotlivých slov a heslo doplňte o čísla a špeciálne znaky.

Napr.: Njatz,vs1Sh.

Príklad 2: Vytvorenie silného hesla nahradením znakov

Vyberte si slovo, ktoré si dobre pamätáte, napr. «popoludnie» a definujte špeciálny reťazec, napr. «1$1». Teraz nahraďte definované časti/písmená slova špeciálnym reťazcom, aby ste vytvorili silné heslo.

Napr. P1$1p1$1ludnie

Upozorňujeme, že na vytvorenie hesla by ste nikdy nemali používať informácie, ktoré sú voľne dostupné v sociálnych médiách. Ďalšie tipy na tému zabezpečenia hesiel môžete získať na našich školeniach o bezpečnosti IT.

5 Referenčné dokumenty

- IS-ISS-GROUP-001-INFORMATION-SECURITY-STRATEGY
- IS-GISP-GROUP-001-GENERAL-INFORMATION-SECURITY-POLICY
- IS-SISD-GROUP-001-PSSS-SPECOPS
- Smernica o používaní IT systémov v spoločnosti Arbonia

6 Nadobudnutie platnosti

Meno	Obchodná jednotka	Funkcia	Dátum	Podpis
Patrick Langenegger	Corporate IT	CIO Arbonia Group / CIO Division Doors	2021-07-08	n/a
Michael Kreter	Division HVAC / Sanitary	CIO Division HVAC / Sanitary	2021-07-08	n/a
Tobias Shibli	Division Windows	CIO Division Windows	2021-07-08	n/a
Reto Knechtle	Corporate IT	Head of IT Infrastructure	2021-07-08	n/a

7 Relevantné prílohy

Č.	Popis	Názov súboru
1	IS-ISP-GROUP-001-COM001-EMPLOYEE-INFORMATION	